Cloud Security using Blowfish and Key Management Encryption Algorithm

B.Thimma Reddy, K.Bala Chowdappa, S.Raghunath Reddy

Abstract— **In the present days security is the major goal in all applications. For securing data in cloud computing there are lot of techniques available. Various disadvantages in cloud are like security, data protection, network security, privacy concerns and are also prone to a variety of attacks like Denial of Service, IP spoofing etc. To overcome these attacks, we can use authentication, authorization, access control and encryption techniques.**

A user can access cloud services as a utility service and begin to use them almost instantly. The fact that services are accessible any where any time lead to several risks. Some of the concerns are lack of confidentiality, integrity and authentication among the users of cloud and service providers. Main goal of my proposal is to provide security in cloud and protecting the data transmitted through various secure channels by providing security using encryption. The cryptographic algorithms like DES, AES, GOST 28147-89, CAST, RC6, SERPENT, and TWOFISH can be adopted for the optimization of data security in cloud computing.

Index Terms— **Blowfish, Key Management. Pervasive Encryption, Cloud Security**

I. INTRODUCTION

The new innovative technology cloud computing facilitates networked nodes to share the pooled resources on demand based on pay per use model. The storage technologies, the sensation of the internet and computing resources are cheaper and are available universally. Resources are of 3 types software as service (Saas), platform as a service (Paas), Infrastructure as a service (Iaas). Some of the services like database as service, storage as service, platform as service and testing as service. Resources like CPU and storage and provided as general utilities to the users on demand through internet. It can handle multitenant request simultaneously and is highly scalable, dynamic, easily configurable, attractive business owners like investment, low operation cost, easy to access, reducing business risks and maintenance expenses. Any user with internet facility can acquire the cloud source according to the service provider's policies and norms at any time without any prerequisites, this creates several security problems and vulnerabilities to the cloud computing environment. We have 3 types of clouds private cloud, public cloud and hybrid cloud. Service providers like AMAZON, APPRENDA, SALESFORCE, CLOUDANT, FABASOFT, RELIACLOUD etc. However from the past few years the cloud computing has made a lot of changes in IT industry even large companies Google, Microsoft are also struggled a lot to provide powerful, cost efficient and reliable cloud platforms. It is more flexible to the users so that many users make use of the cloud leads to various network and information security risks in cloud computing. In cloud computing the client's data is distributed across different networks and stored the client's data in data centers and the data resides in the physical network of service providers. Service providers cover from unexpected security attacks and vulnerabilities when the data is uploaded and offloaded to and from the cloud data centers. Drawbacks for cloud computing is data security, one solutions for this problem is authentication. Security is of 2 types protecting asset and protecting data. We are concentrating mainly on data protection by using cryptographic techniques. By using this cryptographic techniques we are solving some part of security issues in cloud computing.

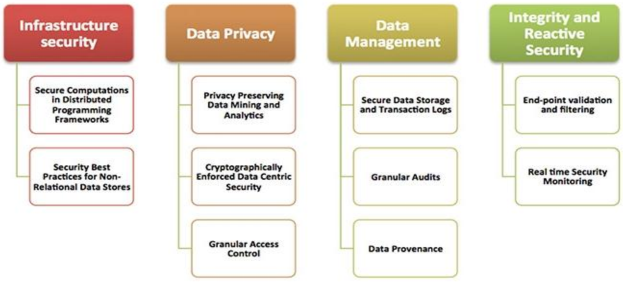

Infrastructure security
Secure Computations in Distributed Programming Frameworks
Security Best Practices for Non-Relational Data Stores
Data Privacy
Privacy Preserving Data Mining and Analytics
Cryptographically Enforced Data Centric Security
Granular Access Control
Data Management
Secure Data Storage and Transaction Logs
Granular Audits
Data Provenance
Integrity and Reactive Security
End-point validation and filtering
Real time Security Monitoring

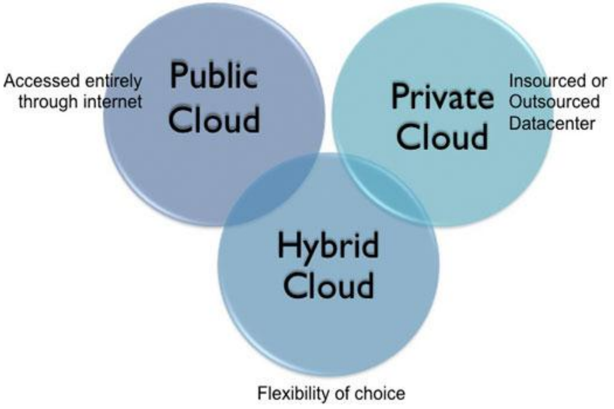
Figure Classification of the Top 10 Challenges

B.Thimma Reddy, CSE Department, G.Pulla Reddy Engineering College, Kurnool.

K.Bala Chowdappa, CSE Department, G.Pulla Reddy Engineering College, Kurnool.

S.Raghunath Reddy , CSE Department, G.Pulla Reddy Engineering College, Kurnool.

2.1 Types of cloud:


Accessed entirely through internet
Public Cloud
Private Cloud
Insourced or Outsourced Datacenter
Hybrid Cloud
Flexibility of choice

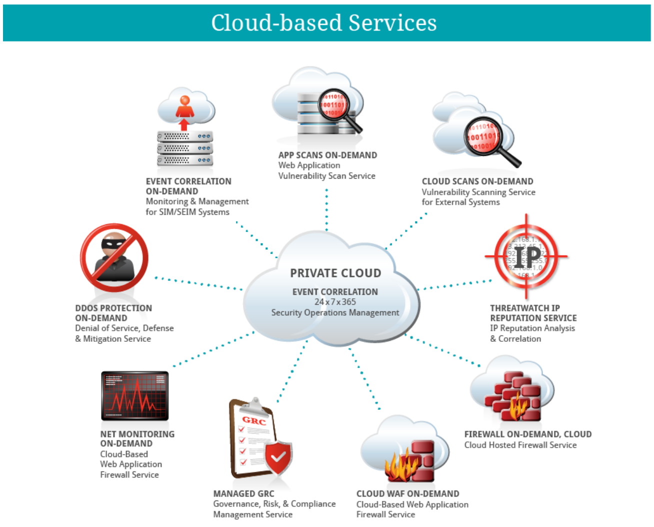
a. Public cloud*:* A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model**.**

b. Private cloud: A private cloud is designed to offer the same features and benefits of public cloud systems, but removes a number of objections to the cloud computing model including control over enterprise and customer data, worries about security, and issues connected to regulatory compliance.

c. Hybrid cloud*:* A hybrid cloud is a cloud computing environment in which an organization provides and manages some resources in-house and has others provided externally.

2.2 Types of cloud services :

a. Software as a Service
b. Platform as a Service
c. Infrastructure as a Service


Cloud-based Services
PRIVATE CLOUD
EVENT CORRELATION
24 x 7 x 365
Security Operations Management
EVENT CORRELATION ON-DEMAND
Monitoring & Management for SIM/SEIM Systems
APP SCANS ON-DEMAND
Web Application Vulnerability Scan Service
CLOUD SCANS ON-DEMAND
Vulnerability Scanning Service for External Systems
DDOS PROTECTION ON-DEMAND
Denial of Service, Defense & Mitigation Service
THREATWATCH IP REPUTATION SERVICE
IP Reputation Analysis & Correlation
IP
NET MONITORING ON-DEMAND
Cloud-Based Web Application Firewall Service
GRC
MANAGED GRC
Governance, Risk, & Compliance Management Service
CLOUD WAF ON-DEMAND
Cloud-Based Web Application Firewall Service
FIREWALL ON-DEMAND, CLOUD
Cloud Hosted Firewall Service

II. PERVASIVE ENCRYPTION

The need for data protection particularly in shared environment and in multi-tenant environments been a primary consideration among customers. In shared environment storage and network resources needs some technologies to protect data in cloud computing, Some surveys identified security is one of the main challenge in implementing cloud computing solutions. Users store sensitive information such as financial data, regulated industries such as health care and public utilities in cloud and cloud will operate external service providers and challenges in achieving security issues. Some solutions are applicable to verify security acquiescence in cloud environment they are inconsistent, scalability, effectiveness. Many organizations deploy their software in fixed hardware infrastructures and noncore applications in the public cloud and some organizations are building their own private clouds.

Some of the security challenges include those of physical layer, virtualization layer and in cloud layer. Security experts mainly concentrate on data isolation issues and address them using pervasive encryption.

III. PERVASIVE ENCRYPTION

Cryptography helps protecting the data from unauthorized access from users and provide security to the data. Data information in cloud environments moves over network among different servers. Repeatedly encrypting and decrypting of data information led to performance tradeoffs that make pervasive encryption undesirable. Using AES encryption algorithm it does affect the performance in pervasive encryption.

a. Aggregated risk

Each physical host is exposed to risk from all the applications and services associated with those virtual machines because many virtual machines execute various times on server

b. Multi-tenancy

After virtualization multi tenancy will lead to Sharing physical resources like memory, processor, database, software's, infrastructure.

c. Resources outside IT control

Creating a dependence on third parties for data protection and control , boundaries between the data center and cloud providers are blurred in public clouds.

IV. ARCHITECTURE AND FRAMEWORK

This security framework for Cloud Computing is based on two algorithms. The concept uses multi-clouds for security purpose so four CSPs are designed for every cloud client to transfer data from one CSP to another.

Algorithm-I:

Integrity verification with Byzantine fault tolerance algorithm This algorithm (BFT) provides safety and liveness over an multi-cloud model.

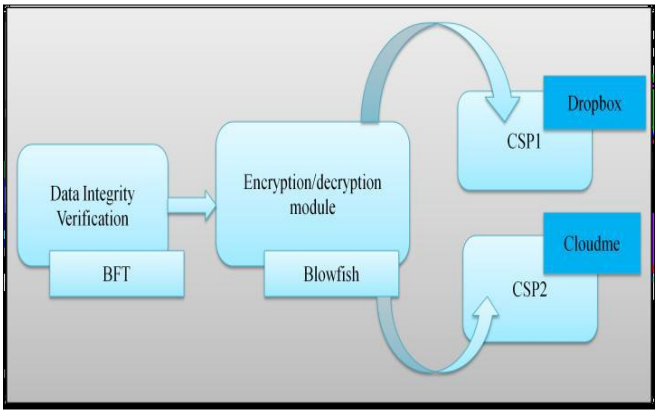
a) **Safety:** The system maintains state and looks to the client like a non-replicated remote service. Safety includes a total ordering of requests.

b) **Liveness:** Clients will eventually receive a reply to every request sent, provided the network is functioning.

It is based on state machine replication and messages signed by public key cryptography. Message digests created using collision-resistant hash functions and uses consensus and propagation of system views: state is only modified when the functioning replicas agree on the change .

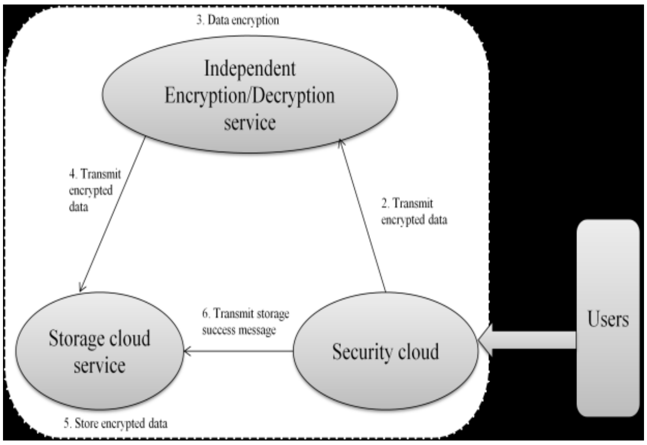
- For n clients, there are n 'views', {0..n-1}.
- In view i, node i is the primary node
- View change is increment mod n
- View change occurs when 2f nodes believe the primary has failed
- Guaranteed safety and liveness provided less than n−14 = f replicas have failed.
- **Step 1:** The client sends a request to the primary cloud.
- **Step 2:** The primary assigns the request a sequence number and broadcasts this to all replicas (pre-prepare).
- **Step 3:** The replicas acknowledge this sequence number (prepare).
- **Step 4:** Once 2f prepares have been received, a client broadcasts acceptance of the request (commit).
- **Step 5:** Once 2f +1 commits have been received, a client places the request in the queue.In a non-faulty client, the request
- queue will be totally ordered by sequence number.
- **Step 6:** Once all prior requests have been completed, the request will be executed and the result sent directly to the client.
- **Step 7:** All these messages are logged.

Algorithm-II: Encryption and decryption with Blowfish algorithm Blowfish uses a ample amount of sub keys. These keys have to be pre-computed afore any abstracts encryption or decryption. The A-array consists of 18 32-bit sub keys : A1, A2,...., A18. There are four 32-bit S-boxes with 256 entries each: S1,0, S1,1,..., S1,255; S2,0, S2,1,..,, S2,255; S3,0, S3,1,..., S3,255; S4,0, S4,1,..,, S4,255. Encryption: Blowfish is a Feistel arrangement consisting of 16 circuit The ascribe is a 64-bit abstracts element, x. Divide x into two 32-bit halves: xL, xR For i = 1 to 16: xL = xL XOR Ai xR = F(xL) XOR xR Swap xL and xR Swap xL and xR (Undo the endure swap.) xR = xR XOR A17 xL = xL XOR A18 Recombine xL and xR Function F (): Divide xL into four eight-bit quarters: a, b, c, and d F(xL) = ((S1,a + S2,b mod 232) XOR S3,c) + S4,d mod 232 Decryption is absolutely the aforementioned as encryption, except that A1, A2,..., A18 are acclimated in the about-face order. Implementations of Blowfish that crave the fastest speeds should disclose the bend and ensure that all sub keys are stored in cache. The subkeys are affected application the Blowfish algorithm. The exact adjustment is as follows: Initialize aboriginal the P-array and again the four S-boxes, in order, with a anchored string. This cord consists of the hexadecimal digits of pi (less the antecedent 3). For example: A1 = 0x243f6a88 A2 = 0x85a308d3 A3 = 0x13198a2e A4 = 0x03707344 XOR A1 with the aboriginal 32 $.25 of the key, XOR A2 with the additional 32-bits of the key, and so on for all $.25 of the key (possibly up to A14). Repeatedly aeon through the key $.25 until the absolute A-array has been XORed with key bits. (For every abbreviate key, there is at atomic one agnate best key; for example, if A is a 64-bit key, again AA, AAA, etc., are agnate keys.) Encrypt the all-zero cord with the Blowfish algorithm, application the sub keys declared in accomplish (1) and (2). Replace A1 and A2 with the achievement of footfall (3). Encrypt the achievement of footfall (3) application the Blowfish algorithm with the adapted sub keys. Replace A3 and A4 with the achievement of footfall (5) Continue the process, replacing all entries of the A- array, and again all four S-boxes in order, with the achievement of the continuously-changing Blowfish algorithm. In total, 521 iterations are appropriate to accomplish all appropriate sub keys.

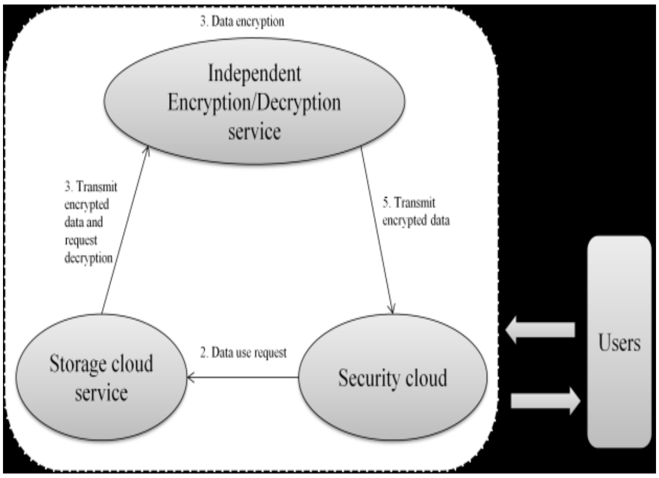


Workflow of a proposed architecture

Data retrieval from cloud service provider: When a user wants to access the online Cloud Service, accept to aboriginal assassinate the Login Program as apparent in step 1. This step can use accepted e-commerce or added casework which accept already deeply absolute the user's registration, such as symmetric key-based claiming and acknowledgment login verification, or through a One-Time Password. After the user's login has been auspiciously verified, if the System requires applicant advice from the user, it sends a appeal for advice to the Storage Service System, as apparent in step 2. In this step, the System transmits the user ID to the Storage Service System area it searches for the user's data. This data is encrypted so, already found, a appeal accept to be beatific to the Encryption/Decryption Service System forth with user ID. step 3 shows the Storage Service System active the manual of encrypted applicant data and the user ID to the Encryption/Decryption Service System. Since the Encryption /Decryption Service System can serve assorted users and the encryption/decryption for anniversary user's data requires a different key, accordingly user's different ID and keys are stored together. Therefore, in step 4, the Encryption/Decryption Service System uses the accustomed user ID to basis the user's data decryption key, which is again acclimated to break the accustomed data. Using the actual decryption key to break the data is analytical to abating the data to its aboriginal state. After the Encryption/Decryption Service System has decrypted the client's data, in step 5 the decrypted user data is provided in step 6, commutable the Data Retrieval Program.


3. Data encryption
Independent Encryption/Decryption service
4. Transmit encrypted data
2. Transmit encrypted data
6. Transmit storage success message
Storage cloud service
Security cloud
Users
5. Store encrypted data

Data storage


3. Data encryption
Independent Encryption/Decryption service
3. Transmit encrypted data and request decryption
5. Transmit encrypted data
2. Data use request
Storage cloud service
Security cloud
Users

Data Retrieval from cloud service provider

TABLE I
THREATS AND SOLUTIONS SUMMARY FOR IAAS

IaaS Component	Threats / Challenges		Solutions	
Service Level Agreement (SLA)	Monitoring and enforcing SLA. Monitor QoS attributes.		Web Service Level Agreement (WSLA) framework. SLA monitoring and enforcement in SOA.	
Utility Computing	Measuring and billing with Multiple levels of providers On-demand billing system availability.		Amazon DevPay.	
Cloud Software	Attacks against XML. Attacks against web services.		XML Signature and XML Encryption. SOAP Security Extensions.	
Networks & Internet connectivity	DDOS Man-In-The-Middle attack (MITM). IP Spoofing. Port Scanning. DNS security.		Logical Network segmentation and Firewalls. Traffic encryption. Network monitoring. Intrusion Detection System and Intrusion Prevention System (IPS).	
Virtualization	Security threats sourced from host: • Monitoring VMs from host. • Communications between VMs and host. • VMs modification.	Security threats sourced from VM: • Monitoring VMs from other VM. • Communication between VMs. • Virtual machines Mobility • Resources Denial of Service (DoS). • VMs provisioning and migration.	Security threats sourced from host: • Trusted Cloud Computing Platform • Terra • Trusted Virtual Datacenter (TVDc) • Mandatory Access Control MAC	Security threats sourced from VM: • IPSec. • Encryption. • VPN. • Xen Security through Disaggregation. • LoBot architecture for secure provisioning & migration VM
Computer Hardware	Physical attacks against computer hardware. Data security on retired or replaced storage devices.		High secure locked rooms with monitoring appliances. Multi-parties accessibility to encrypted storage. Transparent cryptographic file systems. Self-encrypting enterprise tape drive TS1120.	

V. CONCLUSION

It's clear that whereas the use of cloud computing has rapidly developed; cloud computing protection is still considered the main matter in the cloud computing traditional atmosphere. Customers don't need to misplace their private knowledge as a final result of malicious insiders within the cloud. In supplement, the slash of provider availability has initiated many difficulties for a significant quantity of purchasers lately. In addition, data intrusion directs to numerous problems for the customers of cloud computing. In this paper, we have now proposed answers for three most trendy safety threats in cloud storage. We now have confirmed that our approach performs better in decreasing the safety threat on cloud For cloud computing to unfold, customers need to have a high degree of believe in the methods by which provider providers guard their knowledge. This learn proposes a Multi-cloud model for Cloud Computing situated on a Separate Encryption and Decryption service, emphasizing that authorization for the storage and encryption/decryption of user information must be vested with two distinctive carrier providers. On this new model, person knowledge in the Storage provider method is all saved encrypted. Without the decryption key, there is no approach for the provider supplier to access the consumer information. Inside the Encryption/Decryption provider approach there is not any stored consumer data, hence removing the probability that person data probably improperly disclosed.

The info storage security in Cloud Computing, an area stuffed with challenges and of paramount significance, are nonetheless in its infancy now, and plenty of research problems are yet to be identified is to enhance the extra protection points by using making use of different stronger systems of data protection via cryptosystems and other approaches. Cloud computing does provide us with tangible advantages however today we still haven't any definite solutions on a proper protection platform for cloud computing, best recommendations and theories are being fashioned but we're but to see a practical protection measure for cloud computing to be a safer platform for businesses and members.

REFERENCES

[1] Mechanisms to protect data in the open cloud from intel, www.intel.com/opensource/openstack

[2] Cloud security mechanisms for data protection : A survey, International journal of multi media and ubiquitous engineering, vol 9,2014.

[3] Data protection- Aware design for cloud computing, HP labs,2009.

[4] Design and analysis of Data protection as a service for cloud computing, IJCSIT, vol 5 ,2014.

[5] Data security and privacy in cloud computing , Hindawi Publishing Corporation, IJDSN, 2014.

[6] Securing sensitive data for cloud computing from IBM,2013.

[7] A secure frame work for cloud computing with multi cloud service providers, IOSR-JCE vol 17,2015.

[8] Bechtolsheim , A. “Cloud Computing and Cloud Networking.” talk at UC Berkeley, December 2008

[9] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, 34(1), 2011, pp 1-11.

[10] “Cloud security An enterprise perspective” Hewlett-Packard Development Company, L.P. The information, 2012. Available from https://h30613.www3.hp.com/media/files/.../BB237 _Nielson.pdf

[11] O.P. Verma, “Performance analysis of data Encryption Algorithm”, IEEE 3rd International Conference on Electronics Computer Technology (ICECT), vol.5, April 2011, pp. 399-403.

B.THIMMA REDDY is working as an Assistant Professor in the Department of Computer Science and Engineering in G. Pulla Reddy Engineering College (Autonomous): Kurnool, AP, India. He received B.Tech degree in CSE from SKU and M.Tech degree in SE from JNTUA. His areas of interest include Cloud Computing, Big Data.

K.BALA CHOWDAPPA is working as an Assistant Professor in the Department of Computer Science and Engineering in G. Pulla Reddy Engineering College (Autonomous): Kurnool, AP, India. He received B.Tech degree in CSE from JNTUH and M.Tech degree in CSE from JNTUA. His areas of interest include Cloud Computing, Data Mining.

S.RAGHUNATH REDDY is working as an Assistant Professor in the Department of Computer Science and Engineering in G. Pulla Reddy Engineering College (Autonomous): Kurnool, AP, India. He received B.Tech degree in CSIT from SKU and M.Tech degree in SE from JNTUA. His areas of interest include Cloud Computing, Big Data.